Lobachevskii Journal of Mathematics 2016 vol.37 N6, pages 734-739

GCD calculation in the search task of pseudoprime and strong pseudoprime numbers

Dolgov D.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2016, Pleiades Publishing, Ltd.Integer n is called pseudoprime (psp) relative to base a if n is composite, (a, n) = 1, and an−1 mod n = 1. Integer n is called strong pseudoprime (spsp) relative to base a if n is composite, (a, n) = 1, and, ad mod n = 1, or, ad2i mod n = −1, where n −1 = 2s * d, d is odd, 0 ≤ i < s. Pseudoprime and strong pseudoprime numbers are used in public-key cryptography in probabilistic tests. We use recurrent sequences in the task of search pseudoprime and strong pseudoprime numbers. This article describes acceleration of GCD calculation.

http://dx.doi.org/10.1134/S1995080216060111

Keywords

Euclidean algorithm, gcd, Pseudoprime integers, strong pseudoprime, Weber algorithm